AO 106 (Rev. 04/010) Application for Search Warrant AUTHORIZED AND APPROVED/DATE: D.H. Dilbeck 4/30/2025

UNITED STATES DISTRICT COURT

for the

WESTERN DISTRICT OF OKLAHOMA

In the Matter of the Search of *(Briefly describe the property to be search* *Or identify the person by name and address)* IN THE MATTER OF THE SEARCH OF LOCKER #43, PACK-RAT STORAGE, LOCATED AT 2504 SW LEE BOULEVARD, LAWTON, OK 73505	)	Case No: MJ-25-277-CMS

APPLICATION FOR SEARCH WARRANT

I, a federal law enforcement officer or attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following Property *(identify the person or describe property to be searched and give its location)*:

See Attachment A

Located in the Western District of Oklahoma, there is now concealed (*identify the person or describe the property to be seized)*:

See Attachment B

The basis for the search under Fed. R. Crim.P.41(c) is(*check one or more*):

- ☒ evidence of the crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 371	Conspiracy to Commit an Offense Against the United States or to Defraud the United States
18 U.S.C. § 1035	False Statements Relating to Health Care Matters
18 U.S.C. § 1341	Mail Fraud
18 U.S.C. § 1343	Wire Fraud
18 U.S.C. § 1347	Healthcare Fraud
18 U.S.C. § 1349	Conspiracy to Commit Fraud

The application is based on these facts:

See attached Affidavit of Special Agent John Ihle, Defense Criminal Investigative Services, which is incorporated by reference herein.

- ☒ Continued on the attached sheet(s).
- ☐ Delayed notice of [No. of Days] days *(give exact ending date if more than 30 days)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet(s).

Applicant's signature

John Ihle
Special Agent
Defense Criminal Investigative Service

Sworn to before me and signed in my presence.

Date: April 30, 2025

Judge's signature

City and State: Oklahoma City, Oklahoma

CHRIS M. STEPHENS , U.S. Magistrate Judge
Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF OKLAHOMA

IN THE MATTER OF THE SEARCH OF LOCKER #43, PACK-RAT STORAGE, LOCATED AT 2504 SW LEE BOULEVARD, LAWTON, OK 73505	Case No. MJ-25-277-CMS **Filed Under Seal**

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, John T. Ihle, being duly sworn, declare and state as follows:

I. INTRODUCTION

1. I am a "federal law enforcement officer" within the meaning of Federal Rule of Criminal Procedure 41(a)(2)(C), that is, a government agent engaged in enforcing the criminal laws. I have been a federal law enforcement officer since 2013. I have been a special agent with the Defense Criminal Investigative Service (DCIS), Department of Defense Office of Inspector General (DODIG) since January 2023, assigned to the Tulsa Resident Agency. Prior to working for DCIS, I was employed with the United States Army's Criminal Investigation Division's Major Procurement Fraud Unit, assigned to the Dallas Fraud and European Resident Offices from October 2016 to January 2023. Prior to working for MPFU, I was an Active-Duty CID Special Agent with the United States Army's Criminal Investigation Division, assigned to the Fort Sill CID Detachment. I have been the lead case agent on several investigations related to health care fraud, financial crimes investigations, complex

wire fraud schemes, counterfeiting schemes, and money laundering. I have gained experience in the conduct of such investigations through previous case investigations, formal training, and in consultation with law enforcement partners in local, state, and federal law enforcement agencies.

2. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search Locker #43, Pack-Rat Storage, located at 2504 SW Lee Blvd, Lawton, OK 73505, in the Western District of Oklahoma (hereinafter "PREMISES"), further described in Attachment A, for the things described in Attachment B. Upon seizure of the property described in Attachment B, government-authorized persons will review that information. Attachments A and B are incorporated herein by reference.

3. As described more fully below, I respectfully submit there is probable cause to believe that the premises to be searched and items to be seized contain evidence, contraband, fruits, or instrumentalities of criminal violations of 18 U.S.C. §§ 371 (conspiracy to commit an offense against the United States or to defraud the United States), 1035 (false statements related to health care matters), 1341, 1343, 1347, and 1349 (mail, wire, healthcare fraud, and conspiracy).

4. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not purport to set forth all my

knowledge of our investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only.

II. JURISDICTION

5. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

III. STATEMENT OF PROBABLE CAUSE

6. Johnson Medical Consulting D/B/A Combined Home Medical Equipment ("Combined") is a limited liability company formed under the laws of the State of Oklahoma on July 15, 1998. Combined's current business location is an office space located at 2504 SW Lee Blvd, Lawton, OK 73505. My investigation has shown that Linda, Stewart, and Stephen Johnson, are likely in control of Combined.

7. Combined is owned and controlled by the above-mentioned Johnson Family. Linda Johnson is a Registered Nurse in the State of Oklahoma, License #R0025047, and married to Stewart Johnson. Stewart Johnson is a Respiratory Care Practitioner in the State of Oklahoma, License # 3227. Stewart and Linda have three sons, Nathan, Stephen, and Nicholas. All three sons have been employed by

Combined during the suspected fraud scheme and Stephen is currently employed by Combined.

8. Combined currently employees approximately nine employees, recent surveillance has placed several vehicles there, and it currently appears to be open and operational. Vehicles, people, and business activities were observed there as recently as of April 2, 2025.

9. According to the Defense Health Agency ("DHA"), the government health care benefits program TRICARE has processed claims for Combined as recently as March 15, 2025.

10. Evidence obtained thus far includes the following main categories of information:

a. Interviews with witnesses and victims of the current ongoing fraud;

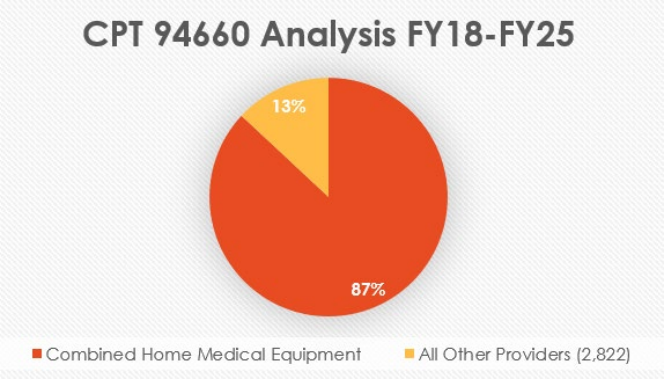
b. Documents provided to agents by victims, banks, healthcare companies, and other witnesses;

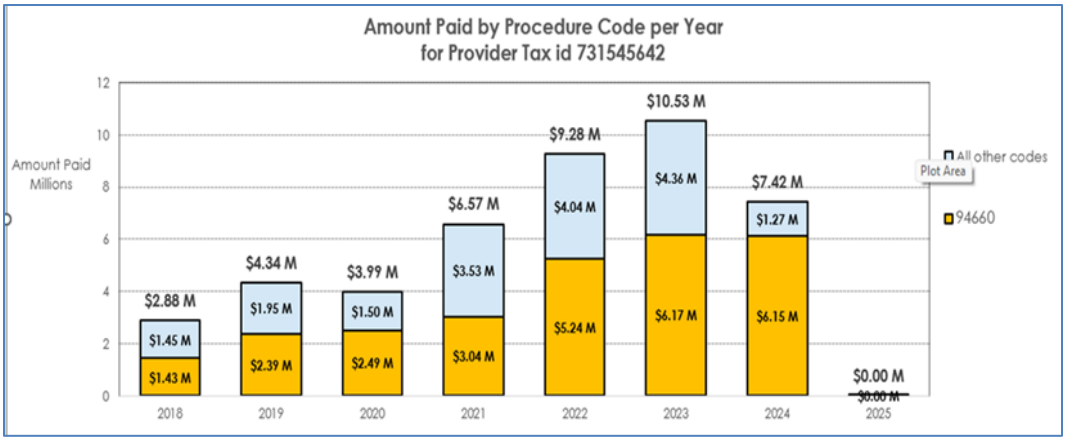
c. Government records involving medical billing to government healthcare benefit programs.

The Current Fraudulent Billing Scheme

11. My investigation has revealed that Combined, which is owned and controlled by Linda, Stewart, and Stephen Johnson, is engaging in a fraud scheme by excessively billing the Current Procedure Terminology (CPT) code 94660 (Continuous Positive Airway Pressure (CPAP) initiation and management). A

Procedure Code Utilization Report for the TRICARE East Region indicated that Combined ranked first overall for the highest paid provider for CPT 94660.





12. According to the DHA, CPT 94660 is intended to be billed for face-to-face encounters between the provider and the beneficiary for either the initial use of a CPAP machine or the management of continuing CPAP use.

13. An audit completed by the DHA contractor Humana Military of medical records indicated allegations of billing excessive units, insufficient documentation, billing for services that were not medically necessary, and billing for services that were not rendered. Face-to-face CPAP discussion between the provider and beneficiary were not documented in the medical records, and the billing of

excessive units especially were not documented. The medical records failed to document compliance reports that are used to substantiate medical necessity. Combined also failed to provide any medical records at all for one claim.

14. A review of Combined's employment records revealed that between January 2018 and September 2024, Combined did not have a medical physician or medical professional who satisfied the provider requirement to bill for CPT 94660. The medical physicians referring the TRICARE beneficiaries for CPAP services were military doctors either on Active-Duty military status or government employees. These referring physicians were not Combined employees, and Combined did not use their National Provider Identifier numbers to bill TRICARE.

The Beneficiary Interviews and Claims Reviews

15. On or about April 1, 2025, B.G., an Active-Duty service member was interviewed at Fort Sill, OK. B.G. stated he received his CPAP machine from Combined on or around February 1, 2023, and has used it routinely to the present time. B.G. has only been to the Combined premises twice. On or around February 1, 2023, when he initially received the machine, and again on or around July 16, 2024, when he picked up supplies for the CPAP machine, B.G. noted an incredible amount of paperwork stacked higher than the computers around the office space of the premises. B.G. explained Combined still utilizes old "dot matrix" printers that print in triplicate and there were piles of their copies all over the office space.

16. A review of the claims data for B.G. showed between February 1, 2023, and June 6, 2024, Combined billed TRICARE 464 times for CPT 94660. This means Combined claimed they saw B.G. face-to-face 464 times over an approximately fifteen-month span. The 464 claims resulted in TRICARE payments of approximately $19,266.

17. On or about April 2, 2025, J.T., a retired military service member was interviewed in Elgin, OK. J.T. stated he received his CPAP machine from the Combined premises on or around September 27, 2019, and used it routinely to the present time. J.T. said he had only been at the Combined premises three or four times over approximately a four-and half-year time frame. J.T. went to the Combined premises the first time to receive his CPAP machine and the subsequent visits were to receive supplies.

18. A review of the claims data for J.T. showed between September 27, 2019, and March 29, 2024, Combined billed TRICARE 1,605 times for CPT 94660. This means Combined claimed they saw J.T. face-to-face 1,605 times over a an approximately four-and-half year time span. Those 1,605 claims resulted in TRICARE payments of approximately $67,432.

19. On or about April 9, 2025, G.C., a retired military service member, was interviewed telephonically while residing in El Paso, TX. G.C. stated he received his CPAP machine from the Combined premises on or around October 9, 2019, and used it routinely. G.C. believed he had been to the Combined premises three or

four times over four or five years. He received his CPAP machine on the first visit and the remainder of the visits were to pick up CPAP supplies. G.C. also stated he was out of the country on a deployment from June 2021 to June 2022.

20. A review of the claims data for G.C. showed between October 9, 2019, and September 2, 2023, Combined billed TRICARE 875 times for CPT 94660. This means Combined claimed they saw G.C. face-to-face 875 times over an approximately four-year time span. Those 875 claims resulted in TRICARE payments of approximately $35,364. Additionally, between June 2021 and March 2022, Combined billed TRICARE for 319 face-to-face visits for G.C. while he was deployed and out of the country. During this specific period of G.C's deployment, TRICARE paid over $13,245 to Combined for face-to-face visits that did not take place.

21. On April 30, 2025, I spoke with Lindee Edwards, the Officer Manager of Combined. She informed me that Combined uses storage locker number 43 at Johnson Ranch LLC, D/B/A Pack-Rat Storage, located at 2504 SW Lee Blvd, Lawton, OK 73505. Pack-Rat Storage was established in 2006 with Linda Johnson listed as the registered agent and shares a commercial address with Combined. Edwards advised that Combined uses locker number 43 to store additional Combined records and property.

22. Because of the above facts, I believe there is probable cause to believe that Combined, as well as Linda, Stewart, and Stephen Johnson, are engaged in

fraud and false statements in violation of numerous federal criminal statutes, and that evidence of this illegal activity is located at the PREMISES.

IV. COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

23. As described above and in Attachment B, this application seeks permission to search for records that might be found on the PREMISES, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

24. *Probable cause.* I submit that if a computer or storage medium is found on the PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear;

rather, that data remains on the storage medium until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

b. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

c. Based on actual inspection of other evidence related to this investigation, including financial records and invoices, I am aware that

computer equipment was used to generate, store, and print documents used in the smuggling scheme. I am also aware based on my knowledge, training, and experience that most TRICARE providers submit claims for reimbursement electronically, using a computer or other electronic device. There is reason to believe that there is a computer system currently located on the PREMISES.

25. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the PREMISES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the

attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can

indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the

computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

26. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained

above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

27. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or

otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

CONCLUSION

28. I submit that this affidavit supports probable cause for a warrant to search the PREMISES described in Attachment A and seize the items described in Attachment B.

Respectfully submitted,

JOHN T. IHLE
Special Agent
DCIS, DODIG

Subscribed and sworn to before me
on April 30, 2025

CHRIS M. STEPHENS
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to be searched

The property to be searched is Locker #43 at Pack Rat Storage, located at 2504 SW Lee Boulevard, Lawton, OK 73505.

ATTACHMENT B

Property to be seized

1. All records relating to violations of 18 U.S.C. §§ 371 (conspiracy to commit an offense against the United States or to defraud the United States), 1035 (false statements related to health care matters), 1341, 1343, 1347, 1349 (mail, wire, healthcare fraud and conspiracy), those violations involving **Johnson Medical Consulting LLC, D/B/A Combined Home Medical Equipment, Linda Johnson, Stewart Johnson, and Stephen Johnson;** and occurring after **January 2018**, including:

A. Records and information regarding healthcare billing and collections;

B. Records and information relating to the e-mail accounts at the "combinedhme.com" domain;

C. Computers or storage media used as a means to commit the violations described above, including 18 U.S.C. §§ 371 (conspiracy to commit an offense against the United States or to defraud the United States), 1035 (false statements related to health care matters), 1341, 1343, 1347, 1349 (mail, wire, healthcare fraud and conspiracy).

2. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in

which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

A. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

B. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

C. evidence of the lack of such malicious software;

D. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;

E. evidence indicating the computer user's state of mind as it relates to the crime under investigation;

F. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

G. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

H. evidence of the times the COMPUTER was used;

I. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

J. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

K. records of or information about Internet Protocol addresses used by the COMPUTER;

L. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

M. contextual information necessary to understand the evidence described in this attachment.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.